UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1988 Volkswagen Vanagon, North Carolina license plate number ECD-8080, registered to Gene Legrand Hickman Jr

Case No. 1:20MJ267-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251	Coercion of a Minor to Engage in Sexually Explicit Activity
18 U.S.C. § 2252A(a)(2)(A)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See Affidavit of Special Agent Gabriela Rees.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Gabriela Rees
Applicant's signature

Gabriela Rees, Special Agent (FBI)
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 09/03/2020 3:26pm

Judge's signature

City and state: Durham, North Carolina

Joe L. Webster, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Gabriela Rees, a Special Agent (SA) with the Federal Bureau of Investigation (FBI) being duly sworn, depose and state as follows:

INTRODUCTION

1. This affidavit is submitted in support of an application for a warrant to search the premises located at 102 Carolina Pines Drive, West End, North Carolina 27376 (the "SUBJECT PREMISES"), and a 1988 Volkswagen Vanagon, North Carolina license plate number EDC-8080, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252A(a)(5)(B) and 2252A(a)(2)(A), which items are more specifically described in Attachment B of this Affidavit.

2. The information contained within this affidavit is based on my training and experience, as well as information I have developed and information relayed to me by other law enforcement agencies. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that instrumentalities, fruits and evidence

of violations of 18 U.S.C. §§ 2251, 2252A(a)(5)(B) and 2252A(a)(2)(A) are located at the SUBJECT PREMISES.

AGENT BACKGROUND

3. I am a Special Agent (SA) of Federal Bureau of Investigation ("FBI"), and have been since October of 2019. I am currently assigned to the Fayetteville Resident Agency of the Charlotte, North Carolina Division. I am assigned to the Violent Crimes Against Children Unit where I am responsible for investigations involving the production, advertisement, receipt, distribution, and possession of child pornography. I am a graduate of the eighteen-week FBI Basic Field Training Course for special agents in Quantico, Virginia. I have received training in the area of child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes. I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256.

4. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252A and 2251,

5. and I am authorized by the Attorney General to request a search warrant.

STATUTORY AUTHORITY

6. This investigation concerns violations of 18 U.S.C. § 2252A relating to material involving the sexual exploitation of minors, and 18 U.S.C. § 2251, relating to the enticement or coercion of a minor to engage in sexually explicit conduct.

a. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported

in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

c. 18 U.S.C. § 2251 prohibits a person from employing, using, persuading, inducing, enticing or coercing a minor to engage in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), for the purpose of producing any visual depiction of such conduct. 18 U.S.C. § 2251(a).

DEFINITIONS

7. The following definitions apply to this application:

a. "Child Pornography," is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Visual Depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. "Sexually Explicit Conduct" refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

d. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

e. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

g. Internet Protocol Address" or "IP Address" is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Secure Hash Algorithm" (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. SHA1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two

or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

i. "Computer" refers to an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

j. "Storage Medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

k. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and

connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

l. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

m. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other

digital form. It commonly includes programs to run operating systems, applications, and utilities.

n. "Records" and "Information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

BACKGROUND ON MAINTAINING CONTRABAND AND STALENESS ISSUES

8. Through my training and experience working cases involving child pornography and though consulting with other experts in the field, I have learned and believe that illegal contraband such as child pornography and other materials like child erotica and incest literature is typically collected, stored and distributed by individuals who trade in this type of illegal activity. This type of contraband (collected child pornography) is not "used up" or consumed as other types of contraband can be such as alcohol or drugs. This type of evidence is usually stored in a manner that is easily accessible to the subject viewing these images and is usually stored on a computer's hard drive

or some other type of accessible electronic storage media, and the images may even be stored off-site via the use of an Internet Service Provider (ISP) and/or a "cloud" type server. Additionally, email and other data files can typically be stored online and is usually only limited by the amount of storage space used by the account holder. A small one (1) inch square object such as a Secure Digital Storage card can literally hold thousands of images.

9. For these reasons contraband of this type can be, and usually is stored for indefinite amounts of time by the possessors of this illegal contraband. In my experience and training, and through consultation with other experts, it is known that in many instances these types of files have been found that were stored for extended amounts of time to include years. These files are transferred from and between storage mediums, and from computer to computer when new computers are obtained by those who collect and trade in child pornography.

10. Computers and the internet allow an individual to collect items and more easily hide their collections from others. The computer has, allowed the individual who views or collects child pornography to maintain a certain anonymity via the internet through the use of non-validated aliases known as "screen names" or "user names", as well as allowing for the storage of the

collection and easy retrieval for viewing. The computer has also made it easy for individuals with similar behaviors or tendencies to contact, exchange information and validate their behavior amongst each other.

11. I know that individuals who view and or collect child pornography, even if viewing these items from an off-site location, generally maintain the ability to view and store these types of items in their residence or what they feel is a secure and easily accessible place, especially through the use of a computer and/or other digital media devices.

12. Because of my training and experience, I know that once a computer file, such as a document or image, is written to the hard drive of a computer, that file or at least traces of that file, can be recovered by forensic analysis techniques even after the file has been "deleted" by the user. These traces can remain on a hard drive for years given the proper circumstances. I also know that files are sometimes written to a hard drive without any overt action by or knowledge of the user.

SEARCH AND SEIZURE OF COMPUTERS AND RELATED MEDIA

13. Based upon my training and experience, and consultations with other law enforcement officers who have been involved in the search of

computers and retrieval of data from computer systems, I know that searching and seizing information from computers often requires law enforcement officers to seize all electronic storage devices (along with related peripherals and stand alone media storage devices) to be searched later by a qualified computer expert in a laboratory or other controlled environment. That process is time consuming and takes days or even weeks. This is true because computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-Roms) can store electronic data which is the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; so, he or she might store it in random order with deceptive file names.

14. While an on-site preview is beneficial to get an initial glimpse of some of the items stored on the media, searching authorities will be required to examine all the stored data to determine which particular files are of evidence or instrumentalities of a crime. This sorting process can take weeks, or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

15. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment.

The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is often difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting procedures designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis. Therefore, removal from the premises of some or all computer equipment and related storage media may be required for proper analysis and specific permission by this search and seizure warrant to remove the computer equipment from the premises and search it over time at a later date is sought.

SPECIAL CIRCUMSTANCES

16. I seek special permission for a forensic examiner, if necessary and technically possible, to acquire a copy of the full digital storage of this device(s) and any attached digital storage mediums as execution of this search warrant,

and to examine such copy for the specific contents described within this affidavit over a necessarily extended period of time, such as is needed to adequately acquire, examine, identify, and seize items of evidentiary value which are likely contained therein. Certain items of digital evidence can require that the device be physically disassembled to allow for data acquisition. Although disassembly may be necessary for evidentiary data to be recovered, it can result in irreversible damage to the use and functionality of the device. Disassembly to this degree for data acquisition will only take place if determined to be necessary by a forensic examiner, and permission to do so will be considered granted upon issuance of this search warrant.

SUMMARY OF THE INVESTIGATION

17. On March 15, 2018, information provided to the National Center for Missing and Exploited Children (NCMEC) by Facebook indicated an adult male user, subsequently identified as Gene HICKMAN (HICKMAN), appeared to be enticing child victims to produce child pornography. Facebook and Instagram provided a total of three tips to NCMEC regarding HICKMAN in March 2018. Subsequent search warrant returns from Facebook revealed HICKMAN was the user of three Instagram accounts and one Facebook

account. HICKMAN described prior incidents of possible child molestation of young boys he "mentored" in chat logs included in the search warrant returns. Due to the context of the chats, "mentored" likely infers sexually grooming minors. Facebook and Instagram chat logs, photos posted by HICKMAN on social media, and an interview of an associate of HICKMAN revealed HICKMAN would often take minors he "mentored" on camping trips in his Volkswagen van. Chat log history and an interview of an identified victim indicate HICKMAN enticed the minor victim to produce child pornography, in violation of Title 18 U.S.C . § 2251. HICKMAN also discussed sexual acts with minors with other Instagram users.

18. Analysis of devices seized from search warrants of HICKMAN's residence on June 5, 2018 and December 12, 2019 revealed HICKMAN also used a Telegram account, and Microsoft OneDrive and Mega for cloud storage. A preliminary review of HICKMAN's Telegram account chat logs revealed HICKMAN likely used Telegram to distribute child pornography, and evidence of child pornography and bestiality were found on HICKMAN's Microsoft OneDrive and Mega cloud storage accounts. HICKMAN also confessed to sexually abusing a minor, in an interview by the Moore County Sheriff's Office on June 5, 2018.

19. HICKMAN was arrested by the Moore County Sheriff's Office on December 19, 2019 and posted bond on June 19, 2020. HICKMAN attempted to contact a previous victim after his release in June, and open source information indicates the phone number used by HICKMAN to contact the victim is associated with Telegram account Gene Hickman Jr, ID 997007914, last online on August 21, 2020.

20. HICKMAN previously used Telegram to distribute child pornography. Evidence obtained from HICKMAN's Telegram account and other devices used by HICKMAN since his release have the potential to identify additional victims of child exploitation and individuals involved in distribution, possession and/ or possible production of child pornography.

21. Seizure of devices found at the SUBJECT PREMISES and inside the 1988 Volkswagen Vanagon, North Carolina license plate number EDC-8080, are being sought to obtain evidence of violations of Title 18 U.S.C. §§ 2251, relating to enticing or coercing a minor to engage in sexually explicit conduct and Title 18 U.S.C. §§ 2252A, relating to material involving the sexual exploitation of minors.

CONCLUSION

22. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of the offense, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES and inside the 1988 Volkswagen Vanagon, North Carolina license plate number EDC-8080, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES authorizing the seizure and search of the items described in Attachment B.

/s/ Gabriela Rees
Gabriela Rees
Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which she submitted to me by reliable electronic means, on this 3rd day of September, 2020, at 3:26pm.

JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

A 1988 Volkswagen Vanagon, North Carolina license plate number EDC-8080.

Photographs attached.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252A(a)(5)(B) and 2252A(a)(2)(A):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);
    b. Records and information referencing child erotica;
    c. Records, information, and items referencing or revealing the occupancy or ownership of 102 Carolina Pines Drive, West End, North Carolina 27376, including utility and telephone bills, mail envelopes, or addressed correspondence;
    d. Records and information referencing or revealing the use of peer-to-peer software, including BitTorrent client software;

e. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

f. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography;

i. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of the Internet Protocol addresses used by the COMPUTER;

e. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

f. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. evidence of the lack of such malicious software;

h. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.